

# Revisionsrapport SITHS och HSA 2014

Version 1.0 2014-09-29

## Innehåll

<b>1. Sammanfattning</b> .....	<b>3</b>
<b>2. Inledning</b> .....	<b>3</b>
<b>3. Bakgrund</b> .....	<b>3</b>
<b>4. Genomförande</b> .....	<b>4</b>
4.1 Urval för revision .....	4
4.2 Revisionsprocessen .....	5
4.3 Metod .....	6
<b>5. Resultat</b> .....	<b>6</b>
5.1 Totalt antal brister per allvarlighetsgrad .....	6
5.2 Resultat för anslutna organisationer .....	7
5.3 Brister per revisionsområde.....	8
5.3.1 Revisionsområde A – HSA .....	9
5.3.2 Revisionsområde B – Kontrollkörningar och stickprovskontroller.....	10
5.3.3 Revisionsområde C – SITHS.....	11
5.3.4 Revisionsområde D – SITHS stickprovskontroll .....	11
5.3.5 Revisionsområde E – Internrevision .....	12
5.4 Resultat för brukarorganisationer till HSA.....	13
5.5 Brister där åtgärder är kopplade till Inera.....	13
<b>6. Analys av resultatet</b> .....	<b>13</b>
<b>7. Analys av genomförande</b> .....	<b>14</b>
<b>8. Bilagor</b> .....	<b>16</b>

### Revisionshistorik

Version	Författare	Kommentar
0.1	Katrine Streng	Första utkast utifrån revisionsrapport godkänd av HSA Förvaltningsgrupp och SITHS PA-grupp
1.0	Katrine Streng	Godkänd av Ansvariga för HSA och SITHS

## 1. Sammanfattning

Inför 2014 års revision av tjänsterna SITHS och HSA valdes totalt tolv organisationer ut att granskas av revisionsutförare hos Inera. Av dessa tolv organisationer var två tjänster (brukarorganisationer till HSA). Revisionen genomfördes med enkätutskick, besök och kompletterande telefonintervjuer.

2014 års revision gjordes inom områdena HSA, Kontrollkörningar och stickprovskontroller inom HSA, SITHS, SITHS Stickprovskontroll samt Intern revision. Fokusområden för besöken var SITHS, inom områdena korthantering, reservkort och funktionscertifikat.

De utvalda organisationerna för revision var; Landstinget Blekinge, Landstinget i Värmland, Mullsjö kommun, Flens kommun, Eda kommun, Falkenbergs kommun, Essunga kommun, Jokkmokks kommun, Stiftelsen Carlanderska sjukhuset, Almaso för tandvården AB samt brukarorganisationerna bokavård.se (Docmondo Sverige AB) och eMortis (Socialstyrelsen).

Resultatet av genomförda revisioner visar på totalt 104 identifierade brister. Av dessa 104 brister bedömdes 39 vara allvarliga, t.ex. att intern revision inte har genomförts samt att SITHS-kort inte spärras för personal som avslutat sin anställning eller att flera organisationer saknar godkänd RAPS.

I respektive organisations revisionsprotokoll ställer HSA och SITHS Förvaltning krav på att den reviderade organisationen ska ta fram en åtgärdsplan för att hantera de identifierade bristerna. Denna åtgärdsplan ska beskriva hur och när bristerna ska hanteras och ska vara Ineras revisionsutförare tillhanda senast 2014-11-15. Enligt beslut tagna i HSA och SITHS Förvaltningsgrupper **ska** samtliga brister som identifieras med prioritet 1 Hög (Allvarlig) vara åtgärdade och inrapporterade till Inera senast sex månader efter att revisionsprotokollet skickats till organisationen för att undvika eskalering och slutligen möjlig avstängning från aktuell tjänst.

Denna rapport presenterar resultaten i sammanfattad form från dessa genomförda revisioner. För fullständiga resultat hänvisas till respektive organisations revisionsprotokoll (bilaga A – L).

## 2. Inledning

Detta dokument beskriver genomförandet och resultatet från revisionen av SITHS- och HSA-anslutna organisationer under 2014. Resultatet har avidentifierats och sammanfattats i denna rapport. De fullständiga resultaten finns i ett revisionsprotokoll för respektive reviderad organisation, bilaga A – L respektive underbilagor. Innehållet i respektive organisations bilaga behandlas konfidentiellt av HSA och SITHS Förvaltning. För att få åtkomst till dessa hänvisas till respektive organisation.

## 3. Bakgrund

HSA och SITHS bygger på tillit, att anslutna organisationer kan lita på att andras information är korrekt och aktuell samt att den information de själva tillgängliggör för andra skyddas på ett bra sätt. I HSA-policyn, som reglerar användandet av HSA, och i SITHS Registration Authority Policy (RAP), vilken reglerar utgivning av tjänsteidentiteter, framgår hur detta ska göras.

I regelverket för HSA och SITHS anges rätten att göra revisioner på anslutna organisationers efterlevnad av respektive regelverk. För att skapa en helhetsbild har HSA Förvaltningsgrupp och SITHS Policy Authority valt att göra gemensamma revisioner. Orsaken till att revisioner genomförs är att bibehålla trovärdigheten hos de båda tjänsterna (HSA och SITHS) samt att öka tryggheten för dem som är anslutna till dessa två tjänster.

Årets revision är den femte i raden av revisioner som genomförs av Inera. Reaktionen från organisationer som tidigare reviderats och anslutna organisationer som fått tagit del av den avidentifierade rapporten har varit övervägande positiva. Arbetet har också uppmärksammats av Myndigheten för samhällsberedskap.

Föregående revisioner har resulterat i ett antal åtgärdsplaner/åtgärdsplaner vilka kontinuerligt följts upp under året. En effekt av revisionerna är en ökad informationskvalitet inom de båda tjänsterna, HSA och SITHS.

Revisionsgruppen har under 2014 bestått av:

- Revisionsansvarig – Katrine Streng, Secure State AB
- Ansvarig SITHS – Jessica Nord, Inera AB
- Ansvarig HSA – Henrika Littorin, Inera AB
- Revisionsresurser – Sandra Jarlö, Secure State AB, Christoffer Johansson, Inera AB och Åsa Berggren, Inera AB

## 4. Genomförande

### 4.1 Urval för revision

Inför 2014 års revision valdes 12 organisationer ut för granskning. Då extern revision till sin natur inte bör vara förutsägbar så finns det inget uttalat regelverk för vilka organisationer som kommer att väljas ut för granskning. Det finns dock riktlinjer som används som underlag för en prioriteringsordning. Denna prioritering sker utifrån följande kriterier:

- Fördelning mellan de olika kategorierna av anslutna organisationer<sup>1</sup>
- Organisationer som inte tidigare har blivit utvalda att granskas i en extern revision
- Organisationer för vilka HSA och SITHS Förvaltning har upptäckt brister under det gångna året, där det finns anledning att befara att informationskvalitet och rutiner är bristfälliga och/eller där Ineras förvaltningar tror att en extern revision skulle kunna

---

<sup>1</sup> Landsting, kommuner, privata vårdgivare, privata HSA- och SITHS-ombud samt brukarorganisationer (tjänster anslutna till HSA)

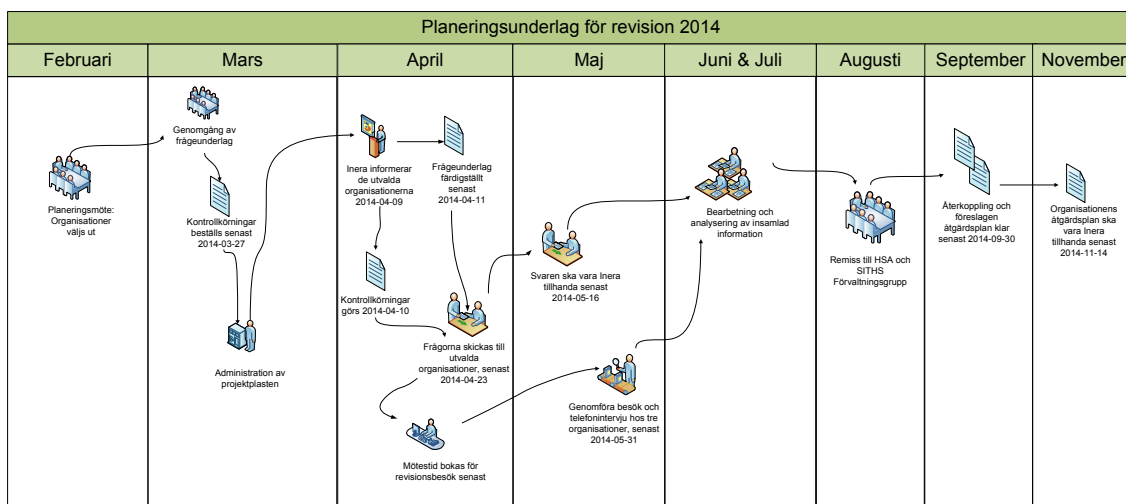
<sup>2</sup> Notera att avvikelser endast betraktas som brist om personer i HSA har angivet uppgifter som inte kan styrkas mot HOSP-registret. Som allvarlig brist betraktas personer som i HSA har felaktigt angiven legitimerad yrkesgrupp

hjälpa ansvariga personer att få arbetet runt HSA och SITHS högre prioriterat i organisationen

2014 har extern revision genomförts på följande anslutna organisationer:

- Landstinget Blekinge
- Landstinget i Värmland
- Mullsjö kommun
- Flens kommun
- Eda kommun
- Falkenbergs kommun
- Essunga kommun
- Jokkmokks kommun
- Stiftelsen Carlanderska sjukhuset
- Almaso för tandvården AB
- bokavård.se (Docmondo Sverige AB)
- eMortis (Socialstyrelsen)

## 4.2 Revisionsprocessen



De utvalda organisationerna kontaktades och informerades om att de blivit utvalda för revision samt hur revisionen skulle genomföras. Parallellt tog revisionsansvarig fram ett revisionsfrågeunderlag som förankrades med ansvariga för SITHS och HSA och som därefter skickades ut till respektive organisation i form av en webbenkät. För de organisationer som valts ut för besök respektive telefonintervju bokades tid för detta.

Dessutom genomfördes kontrollkörningar på valda delar av HSA-innehållet och resultatet av dessa publicerades i behörighetsstyrda mappar på Projektplatsen dit ansvariga i respektive organisation fick åtkomst för att kunna kommentera resultatet i enkäten. Dessa körningar gjordes inte för brukarorganisationerna. En stickprovskontroll gjordes detta år även för SITHS.

De besvarade enkäterna samt dokumentationen vid besöksrevisionerna och telefonintervjuerna har resulterat i ett revisionsprotokoll för respektive organisation där identifierade brister beskrivits och bedömts ur allvarlighetsynpunkt. Revisionsprotokollen innehåller även förslag på lämpliga åtgärder som organisationen bör vidta för att rätta till dessa brister.

### 4.3 Metod

Revisionen för SITHS respektive HSA genomfördes huvudsakligen med enkätutskick (bilaga M) och kontrollkörningar. För brukarorganisationerna användes anpassade enkäter då de inte är anslutna till SITHS och inte publicerar information i HSA. Som komplement till enkäten genomfördes även besök hos och telefonintervjuer med utvalda organisationer. Besöken fokuserade till större delen på den praktiska SITHS-hanteringen, medan telefonintervjuerna främst användes för att utveckla och förtydliga organisationens enkätsvar.

## 5. Resultat

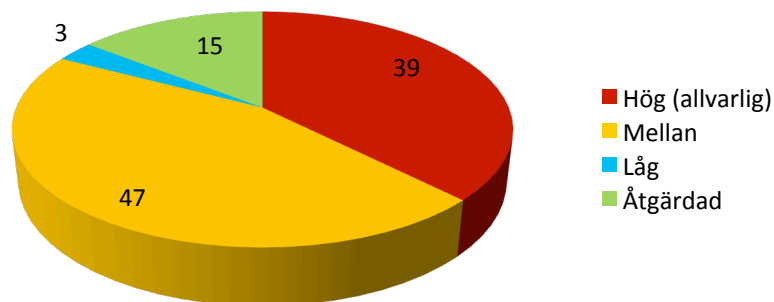
I detta kapitel redovisas de brister som identifierats under revisionen. Bristerna som identifierats är bedömda utifrån vilken allvarlighetsgrad som bristen har enligt följande fyrgradiga skala där bristen bedöms som:

1. Hög (allvarlig) – röd  
Om organisationen inte har uppfyllt regelverket, om bristen är omfattande eller allvarlig vad gäller kvalitetssäkrings- eller identifieringsrutiner har bristen bedömts som allvarlig och getts hög prioritet att åtgärda.
2. Mellan – gul  
Om organisationen endast delvis har uppfyllt regelverket, om bristen är begränsad i omfattning och allvarlighetsgrad har bristen bedömts med mellan prioritet.
3. Låg – blå  
Om organisationen i stort har uppfyllt regelverket men behöver göra mindre justeringar eller kontroller har bristen bedömts med låg prioritet.
4. Åtgärdad – grön  
Brister som identifierades i de kontrollkörningar och stickprov som Inera gjorde och även i de kontroller som organisationerna i enkäten ombads att göra på egen hand men som redan åtgärdats av organisationen när resultatet av revisionen sammanställdes.

### 5.1 Totalt antal brister per allvarlighetsgrad

Sammanlagt har 104 brister identifierats under revisionen 2014. Fördelningen per allvarlighetsgrad visas i cirkeldiagrammet nedan.

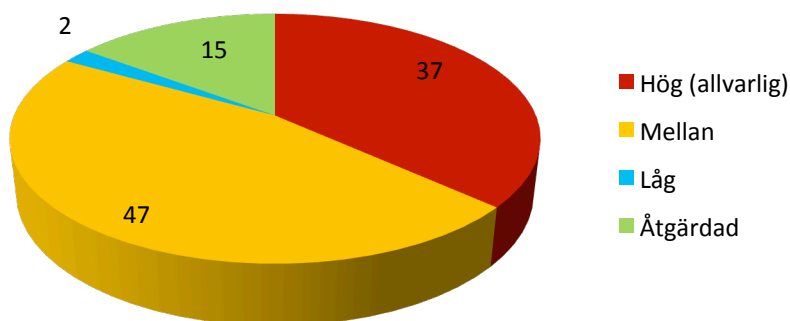
## Totalt antal brister (104 st) fördelning per allvarlighetsgrad



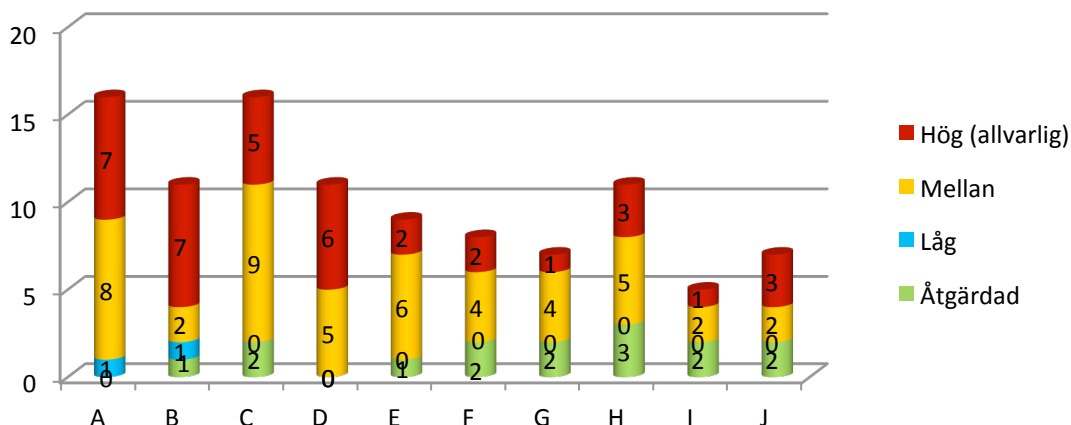
### 5.2 Resultat för anslutna organisationer

För anslutna organisationer identifierades 101 brister totalt, varav 37 bedömdes vara av allvarlig karaktär. Fördelningen per ansluten organisation redovisas nedan.

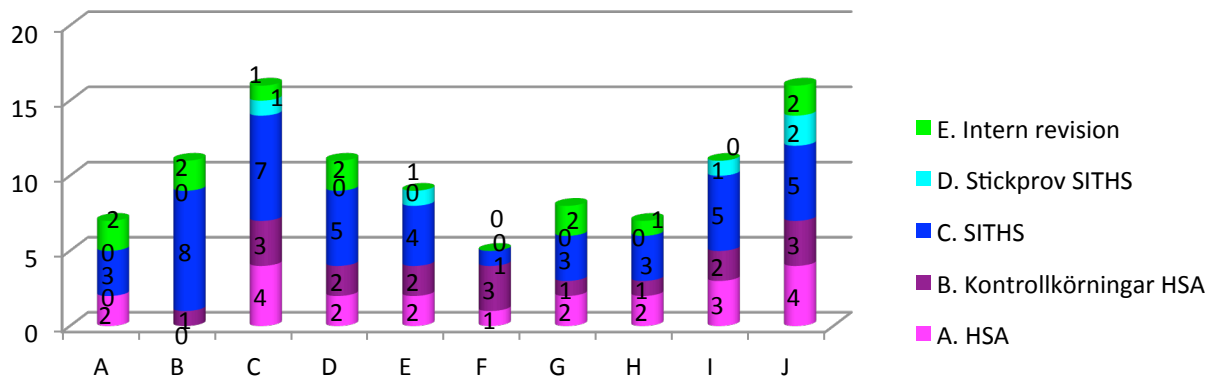
## Brister anslutna organisationer (101 st) fördelning per allvarlighetsgrad



## Totalt antal brister per organisation (fördelat per allvarlighetsgrad)



## Totalt antal brister per organisation (revisionsområde)



### 5.3 Brister per revisionsområde

Diagrammet nedan illustrerar antalet brister inom respektive revisionsområde;

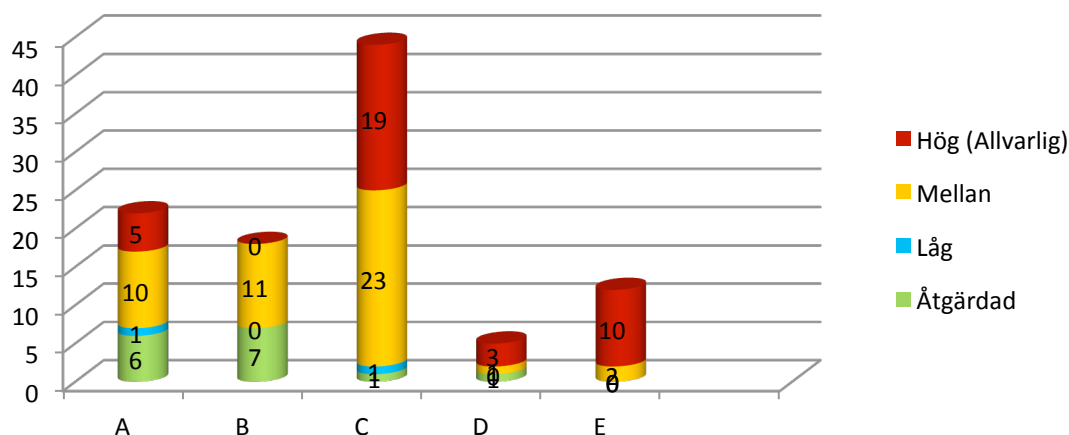
- A = HSA
- B = Kontrollkörningar och stickprovskontroller
- C = SITHS



- D = SITHS Stickprovskontroll
- E = Intern revision

Brister som identifierades under revisionsbesöken samt telefonintervjun har placerats in under respektive område i enkäten och redovisas inte separat.

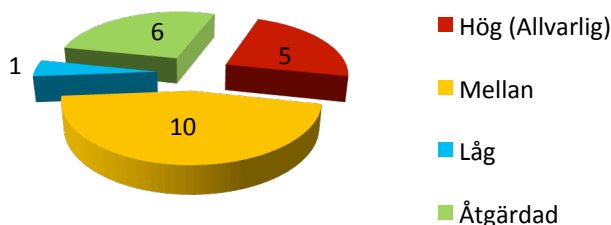
## Brister per revisionsområde



### 5.3.1 Revisionsområde A – HSA

Inom detta revisionsområde identifierades totalt 22 brister, varav 5 bedömdes vara allvarliga.

## HSA totalt 22 brister



Följande allvarliga brister identifierades:

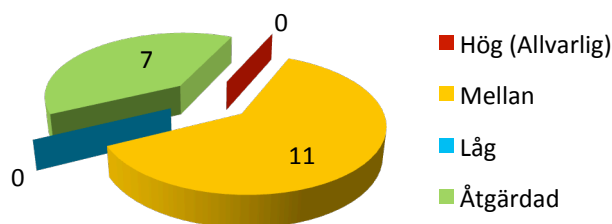
- Rutinbeskrivning för hur kontroll sker av personers anställnings-/uppdragsförhållanden saknas
- Kontroll av personers anställnings-/uppdragsförhållande sker inte enligt HSA-policyns krav (förekom hos två organisationer)

- Uppgifter för personer som är registrerade i HSA avviker från uppgifter i HOSP-registret<sup>2</sup>
- Vårdenhet som upphört med sin verksamhet har ej arkiverats utan istället tagits bort

### 5.3.2 Revisionsområde B – Kontrollkörningar och stickprovskontroller

Inom detta revisionsområde identifierades totalt 18 brister. Inga brister inom området bedömdes som allvarliga.

#### Kontrollkörningar HSA totalt 18 brister

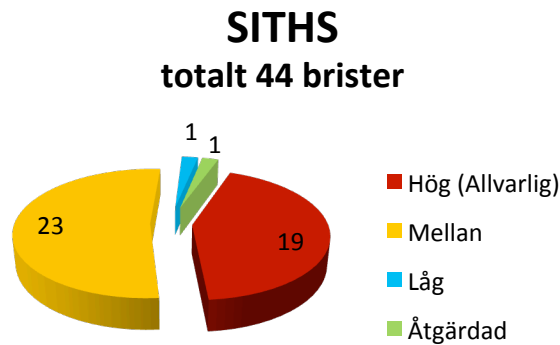


---

<sup>2</sup> Notera att avvikelser endast betraktas som brist om personer i HSA har angivet uppgifter som inte kan styrkas mot HOSP-registret. Som allvarlig brist betraktas personer som i HSA har felaktigt angiven legitimerad yrkesgrupp och/eller förskrivarkod då dessa uppgifter kan leda till att personen obehörigen ges åtkomst till känslig patientinformation.

### 5.3.3 Revisionsområde C – SITHS

Inom detta revisionsområde identifierades totalt 44 brister, varav 19 bedömdes vara allvarliga.



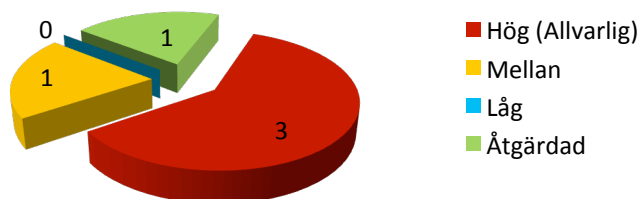
Följande allvarliga brister identifierades:

- RAPS är inte godkänd (förekom hos fem organisationer)
- Rutinbeskrivning av identifieringsrutin vid beställning och utlämning av kort saknas
- Rutinbeskrivning av intygsgivning saknas
- Rutinbeskrivning av kvittensprocessen saknas
- Rutinbeskrivning av arkiveringsprocessen saknas
- Otillåten id-handling används i identifieringsprocessen vid beställning och utlämning av SITHS-kort (förekom hos två organisationer)
- Felaktig rutin för avregistrering av SITHS-kort. När HSA-ansvarig tar bort personposten i HSA innan SITHS-certifikat avregistrerats kan inte tredjepartsleverantör av SITHS avregistrera certifikatet
- Felaktig kvittensrutin gällande reservkort då dessa alltid ska kvitteras med papperskvittens
- Felaktigt id-sätt har använts vid utgivning av reservkort
- Fel persons id-handling registreras i SITHS Admin vid distansutgivning av reservkort (förekom hos tre organisationer)
- Ej utgivna SITHS-kort förvaras obevakade vid ett oläst utlämningsställe
- RA och ORA har åtkomst till både funktionscertifikat och tillhörande koder

### 5.3.4 Revisionsområde D – SITHS stickprovskontroll

Inom detta revisionsområde identifierades totalt 5 brister, varav 3 bedömdes vara allvarliga.

## Stickprovskontroll SITHS totalt 5 brister



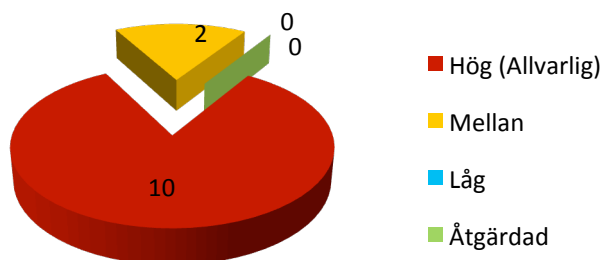
Följande allvarliga brister identifierades:

- Efterfrågade kortkvittenser saknas (förekom hos två organisationer)
- Samma reservkort har lämnats ut till flera olika personer i produktionsmiljö (skarp miljö)

### 5.3.5 Revisionsområde E – Internrevision

Inom detta revisionsområde identifierades totalt 12 brister, varav 10 bedömdes vara allvarliga.

## Intern revision totalt 12 brister



Följande allvarliga brister identifierades:

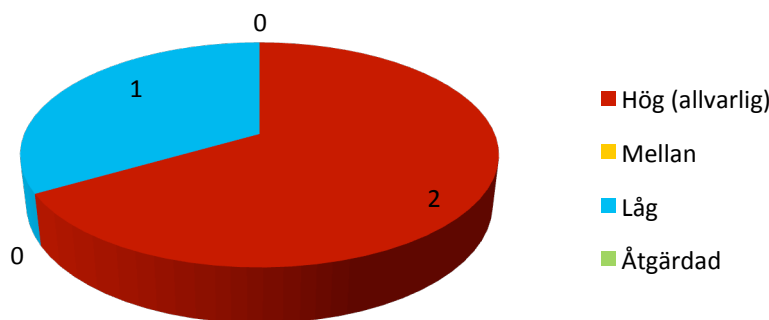
- Ingen intern revision har genomförts gällande HSA de senaste 12 månaderna (förekom hos fyra organisationer)
- Ingen intern revision har genomförts gällande SITHS de senaste 12 månaderna (förekom hos fyra organisationer)

- Inget dokument har laddats upp i enkäten som påvisar genomförd internrevision gällande SITHS, varpå det inte kan styrkas att internrevision har genomförts de senaste 12 månaderna
- Den senaste genomförda internrevisionen gällande SITHS har inte genomförts på ett korrekt sätt och är därmed inte godkänd som genomförd intern revision

## 5.4 Resultat för brukarorganisationer till HSA

Totalt identifierades 3 brister hos de utvalda brukarorganisationerna. Av dessa brister ansågs 2 brister vara allvarliga.

### Brister brukarorganisationer (3 st) fördelning per allvarlighetsgrad



Följande allvarliga brister identifierades:

- Den juridiska utredningen kring hantering av personer med skyddade personuppgifter som enligt avtalet skulle genomföras under våren 2013 är inte genomförd
- Personer med skyddade personuppgifter hanteras på samma sätt som övriga personer utan att riskerna med detta har utretts

## 5.5 Brister där åtgärder är kopplade till Inera

Under 2014 år revision har inga brister med åtgärder kopplade till Inera identifierats.

## 6. Analys av resultatet

Årets revision har genererat ett mindre antal brister jämfört med tidigare år. Vi tror att en väsentlig anledning till detta är införandet av ny HSA-policy och ny RA-policy under 2013 och det efterföljande arbetet med att kontrollera att samtliga anslutna organisationer inkommer med uppdaterade anslutningsdokumentation (HPTA och RAPS). Dels har kraven i policyn

uppmärksammats på nytt, dels har den tidigare vanliga bristen om avsaknad av eller brister i anslutningsdokumentationen i stort sett eliminerats gällande HSA.

För första gången har vi även en organisation utan identifierade brister med i revisionen.

En mycket positiv skillnad från tidigare år är att andelen brister som redan åtgärdats vid sammanställningen av revisionsresultatet har fördubblats. Det vi tyvärr också kan se är att andelen brister som bedöms som allvarliga också har ökat. Antalet brister inom området HSA har minskat radikalt, vilket till största delen torde bero på arbetet med uppdaterad anslutningsdokumentation.

Det största problemet som uppdagats under revisionen detta år är att det finns aktiva SITHS-certifikat kvar när personen som certifikatet är utgivet till har avslutat sin anställning eller sitt uppdrag. Denna brist har identifierats hos 9 av 10 anslutna organisationer. Vi rekommenderar därför att denna fråga kvarstår till nästa års revision och även får särskilt utrymme i informationsaktiviteter under det kommande året.

Den vanligaste bristen från tidigare revisioner av granskade organisationer var att internrevisioner ej genomförts. Detta ser vi har blivit något bättre, men tyvärr är bristen fortfarande relativt vanligt förekommande. Att genomföra internrevision är ett viktigt verktyg för en ansluten organisation. Att i samband med en internrevision identifiera brister i informationskvalitet och rutiner är starkt bidragande till en bättre och säkrare hantering av de båda tjänsterna. Vi anser att det är viktigt att även denna fråga kvarstår i nästa års revision.

En av de anslutna organisationerna har fått ett stort antal brister med hög allvarlighetsgrad eftersom de inte besvarat revisionsfrågorna. Istället för att ta hjälp av sitt ombud att besvara frågorna har de endast hänvisat till att de har ett SITHS-ombud. För att undvika denna typ av – möjligen helt onödiga – brister behöver vi bli ännu mer tydliga gentemot de organisationer som granskas att de ska ta hjälp av sitt ombud och besvara samtliga frågor i enkäten.

## 7. Analys av genomförande

Under arbetet med den externa revisionen 2014 har vi fått många erfarenheter som kommer att förbättra arbetet i framtiden.

Revisionsbesöken var som vanligt mycket givande, både för oss revisorer och för representanterna från de granskade organisationerna. Det vi konstaterat i år är att antalet brister som identifierades vid besöken är förhållandevis få. Det kan visa på att vi nu arbetat fram ett bra frågebatteri i enkäterna som gör att vi fångar upp de flesta bristerna redan där. Men det finns fortfarande ett stort värde i att fortsätta att genomföra revisionsbesök hos några utvalda organisationer varje år. Dels för att vi under dessa besök identifierar brister som vi inte skulle kunna fånga upp i en enkät. Men också för att organisationen ges en möjlighet till dialog både under revisionsdiskussionen men även inom andra områden som normalt inte hanteras inom revisionen, vilket upplevs positivt från de utvalda organisationerna som har fått besök från Inera.

Telefonintervju var även det ett bra verktyg. Det är även ett mer ekonomiskt och miljövänligt alternativ till besök. Dock bör tekniken säkerställas innan intervjun för att inte onödiga hinder skall uppstå. Man bör exempelvis med fördel kunna nyttja videokonferens framför traditionell telefonkonferens där så är möjligt.

Under genomförandet kom även revisionsgruppens eskaleringsplan att nyttjas i ett tidigt skede. En organisation informerades i enlighet med eskaleringsplanen om de följder som skulle kunna komma att träda i kraft om inte korrigeringar i deras svar på revisionen skickades in. Efter att informationen gått ut skickade organisationen in en ny version av enkätsvaret med mycket bättre kvalitet.

## 8. Bilagor

Bilagorna A – L innehåller fullständiga revisionsprotokoll för respektive organisation. Utöver revisionsgruppen, HSA förvaltning och SITHS förvaltning på Inera är det endast medlemmarna i SITHS PA-grupp och HSA Förvaltningsgrupp har behörighet att erhålla dessa från Inera.

Bilaga	Namn	Kommentar
A	Bilaga A Revisionsprotokoll A	Konfidentiell
B	Bilaga B Revisionsprotokoll B	Konfidentiell
C	Bilaga C Revisionsprotokoll C	Konfidentiell
D	Bilaga D Revisionsprotokoll D	Konfidentiell
E	Bilaga E Revisionsprotokoll E	Konfidentiell
F	Bilaga F Revisionsprotokoll F	Konfidentiell
G	Bilaga G Revisionsprotokoll G	Konfidentiell
H	Bilaga H Revisionsprotokoll H	Konfidentiell
I	Bilaga I Revisionsprotokoll I	Konfidentiell
J	Bilaga J Revisionsprotokoll J	Konfidentiell
K	Bilaga K Revisionsprotokoll K	Konfidentiell
L	Bilaga L Revisionsprotokoll L	Konfidentiell
M	Bilaga M Revisionsfrågor HSA och SITHS 2014	Se <a href="http://www.inera.se/hsa">www.inera.se/hsa</a> under Dokument och Revisionsmaterial
N	Bilaga N Sammanställning brister samt diagram 2014	Konfidentiell